



# CVE-2017-5495

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2017-5495
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-01-24 07:59:00 UTC
<b>Updated</b>	2018-01-05 02:31:00 UTC
<b>Description</b>	All versions of Quagga, 0.93 through 1.1.0, are vulnerable to an unbounded memory allocation in the telnet 'vty' CLI, leading

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Quagga</a>	<a href="#">Quagga</a>	All	All	All	All

## References

Reference	Source
lib: limit size of vty buffer to 4096 bytes by qlyoung · Pull Request #63 · FRRouting/frr · GitHub	CONFIRM
Quagga CVE-2017-5495 Denial of Service Vulnerability	BID
Quagga Routing Software - News: Quagga 1.1.1 Released [Savannah]	CONFIRM
[quagga-dev 16560] CVE-2017-5495 text	CONFIRM
Quagga vty_write() Buffer Memory Allocation Flaw Lets Remote Users Cause the Target Service to Crash - SecurityTracker	SECTRACK
Red Hat Customer Portal	REDHAT
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500596](#) Alpine Linux Security Update for quagga

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)